COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, CHAIRMAN

NEWS RELEASE

For Immediate Release:
February 16, 2005

Contact: Robert White/Drew Crockett
(202) 225-5074

Davis Statement on 2004 Federal Computer Security Report Card Grades

Washington, D.C. – Government Reform Committee Chairman Tom Davis (R-VA) issued the following statement today on the 2004 Federal Information Security Management Act (FISMA) report card grades:

"Today, there's good news and bad news. The good news is, the grade for government agencies overall rose 2.5 points last year. The bad news is, the overall grade is a D+. The 2004 FISMA grades indicate that agencies have made significant improvements in certifying and accrediting systems, annual testing, and security training, but significant challenges remain.

"Our committee's primary goal is to help create a 21st century government to meet 21st century challenges and fight 21st century enemies. Our optimal weapon in this struggle is information. Information moved within agencies and across departments. And information moved across jurisdictions of government as well. Seamlessly. Efficiently. SECURELY. Given the interconnectivity of systems across cyberspace, all it takes is one weak link to break the chain.

"As I noted earlier, there's good news and bad news today. Several agencies continue to receive failing grades, and that's unacceptable. The committee will continue to explore the reasons these agencies continue to under-perform; after all, the "goal posts" have not moved significantly over the past several years. On the good news front, we're also seeing some exceptional turnarounds. The Department of Transportation, which received an A-, should be commended for the tremendous security improvement it accomplished this year, most notably in the area of certification and accreditation. Other agencies that deserve commendation may not have received As, but they have achieved large score increases. They've covered a lot of ground in a short period of time. For instance, while the State Department's grade only increased to a D+, I think it's important

to acknowledge their accomplishments this year; they earned a 30 point gain in their score, and are only a half point away from a C.

"Despite these advances, there are still areas throughout the Federal government that need improvement. They are: annual review of contractor systems; testing of contingency plans; configuration management; incident reporting; specialized training for employees with significant security responsibilities.

"The grades are a helpful way for Congress to gauge an agency's information security progress, but this is by no means an exact science. There are several challenges to achieving precise results. For instance, while many IGs do an excellent job completing the FISMA annual independent audits, sometimes the assessment process is hampered when IGs submit incomplete reports or fail to submit anything at all. However, there is clearly a need for the IGs to standardize their evaluation process in order to ensure the accuracy of their reports and to ensure that we can make fair comparisons between the agencies.

"The people on the frontlines – the CIOs, CISOs, and their staff – have to believe in what they're doing. We need to give them the tools, budget, and training they require. I'm proud to announce the formation of the industry-led CISO Exchange, a public-private initiative focused on empowering CISOs to improve Federal Government IT security. The CISO Exchange will convene quarterly educational meetings to encourage the exchange of ideas and best practices between government and private sector information security professionals, as well as produce an annual report on Federal IT Security priorities and operational issues. While this program will be informal and not something we're creating in statute, it's conceptually consistent with what I've done with the Digital Tech Corps, and the proposed Acquisition Workforce Exchange Program – the goal being cross-pollination of ideas and best practices between the private and public sectors.

"I realize the FISMA process is not a perfect one. I think it provides the agencies with a strong management framework, but I recognize that it is not a panacea; there may be a need for amendments to facilitate implementation of the security concepts that drive FISMA. We look to the CIOs and CISOs to help improve the process. We want to hear from them about what challenges they face; what additional resources they may need; and what they think Congress can do to help. Ultimately, we want to ensure that FISMA compliance does not become a paperwork exercise where agencies comply with the letter, but not the spirit, of the law. We don't want them filling out forms to simply fill out forms."

###